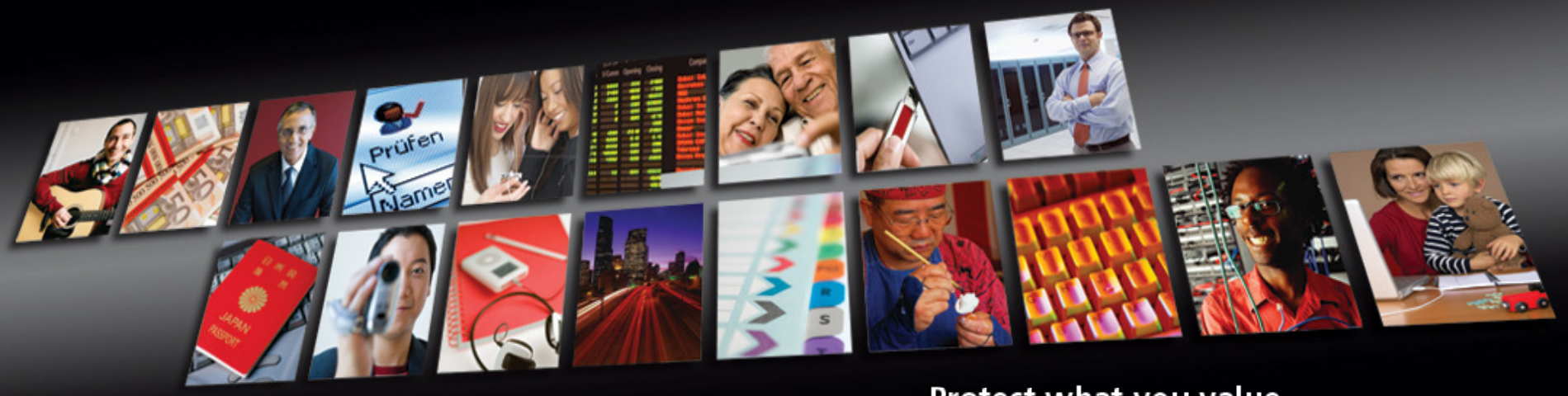
McAfee



SCAP - A Look Ahead

Maturing for the Future

Kent Landfield

Director, Risk and Compliance Security Research

Agenda

- What is SCAP
- What SCAP is Not
- SCAP Use Cases
- Short Term Items to Address
- CVSS fits where???
- Patch Content Needs
- SCAP Going Global
- Content QA
- Content Lifecycle Tools
- What is needed to improve SCAP?
- How SCAP Can Change Auditing

What is SCAP ?

SCAP is a suite of selected open standards that enumerate software flaws, security related configuration issues, and product names; measure systems to determine the presence of vulnerabilities; and provide mechanisms to rank (score) the results of these measurements in order to evaluate the impact of the discovered security issues. SCAP defines how these standards are combined.

What SCAP Is Not ?

- A single Protocol
- Serving a single use case
- A Federal Government only standard
- Only exists to support FDCC
- A compliance only set of standards
- A US-only standard

SCAP Use Cases

- **Policy and Compliance Validation (primary focus today)**
- Vulnerability Detection
- Asset Management
- Risk Monitoring and Response
- Security Products Producer / Consumer
- Threat Publishing and Alerts
- Others …

Short Term Items to Address

- Inconsistency between level of documentation within SCAP Standards
  - Specifications vs Schemas as documentation
  - All component standards need to be documented
- Inconsistent use of terms between standards
  - One document uses “properties” and another uses “entities”
  - Common terminology and uniformity lacking
- Lifecycle approach to SCAP development
- Specific documentation needed to fill in the usage gaps between standards
  - Lack of Integration documents between XCCDF and it’s checking engine component standard
- Provide a mechanism for the community to assist
  - Wiki/Twiki maybe

CVSS fits where???

- CVSS sits on the sidelines today underutilized
- Not one of the XCCDF Scoring models
- No specified way to integrate it with the associated CVE in OVAL content
- We need integrate it so it can be used in scoring
- And now we are taking about CCSS? …

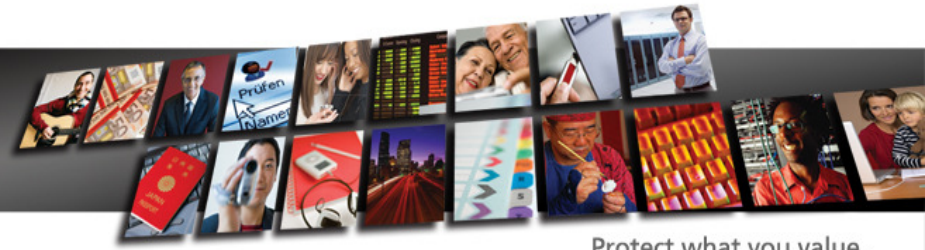
Patch Content Needs

- Policy driven “PatchesUpToDate” usage
  - Lots of problems supplying this in its current form
  - OVAL 5.5 will assist
- Security and Operational Patch Needs
  - A MS Bulletin Benchmark
  - A Red Hat Errata Benchmark
  - Tailoring aspects

SCAP Going Global

- Need to address I18N/L10N
  - Critical if the government truly wants COTS and GOTS solutions
- Localization of content
  - XCCDF and CPE support it
  - OVAL does not
  - CVE has limited translations
  - Others don't
- Need to deal with not just the translations
  - Translations are a presentation issue
  - Need to be able to assess a locale specific system accurately even if the presentation is in English
- And then there are GEO specific policies that need to have benchmarks created for them
  - ACSI 33, J-SOX, EU 8th Company Law Directive on Statutory Audit, etc.

This is coming sooner than most realize…



Content QA

- So who is doing QA on public content?
- Where do we find out the tested status of the content?
- The old ways of throwing VM images and systems at the problem down work
- Re-architect the approach to QA of content using language provided capabilities
  - System Characteristics files
- Automated testing is not only doable, but it is not that complicated or costly

Content Lifecycle Tools

- Home grown or Oxygen type today
- Individual vendors are actively developing SCAP Content Management environments and tools for their specific products
- These efforts include
  - SCAP Content Database
  - Content Revisioning and Publishing,
  - Content Developer Tools
  - QA Testing Support
  - Automated Testing Framework
- For content developers the needed infrastructure and tools are critical

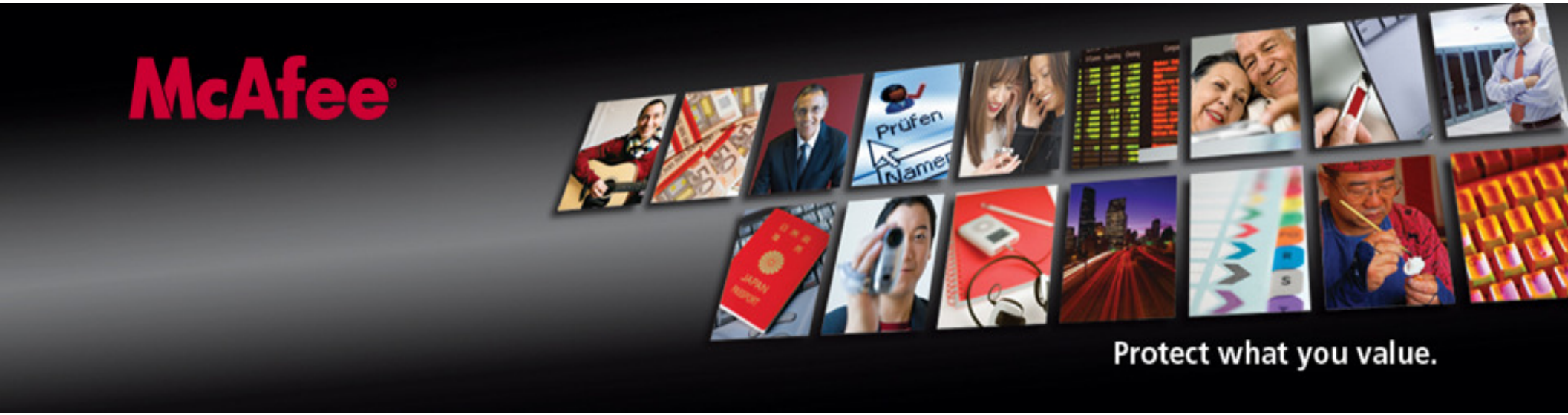
What is needed to improve SCAP?

- CVSS needs to integrate with the other SCAP component standards
- Enterprise reporting standards
  - Organizational-wide reporting
  - Common Results Formats
  - Risk Metrics / Peer comparison
- Security Model for SCAP
- Content Signing capabilities
- Much better documentation about each and every component standard
- Better tools and Content Management infrastructure
- Database support
- Content Repository and Distribution Standards
- A global view of it's long term usage

How SCAP Can Change Auditing

In a future not so far away…

- IT / Operations /Security will not have to stop what they are doing to prepare for an external audit
- Auditors will not need to bring in their own tools to audit the network assets directly
- Signed Benchmarks approved by the Auditor are running on the network
- IT staff hands the auditor the signed benchmark, the signed tailoring settings file and access to the signed results files.
- The auditor can the review the benchmark and the results, verify the signatures and determine if there are areas that the site should be validating / auditing that they currently are not and makes benchmark improvements.
- Their improvements are then put in place and now additional items are validated.
- Operations and management now have a continuous view of the status of there network…



Kent Landfield
Kent_landfield@mcafee.com
Office: 972.963.7096
Mobile: 214.385.1138